The Commonwealth of Massachusetts, Department of Mental Health

Security and Confidentiality for DMH Computerized Information Systems containing Client Records or Data

Policy # 98-6

Date of Issue: July 17, 1998

Effective Date: July 17, 1998

Replaces Policy #: 95-6

Approval by Commissioner

Signed by: Marylou Sudders

Date: July 17, 1998

I. PURPOSE OF POLICY:

This policy establishes specifications for safeguarding the confidentiality of Department of Mental Health (DMH) Client Records and Data stored in DMH Computerized Information Systems. This policy replaces DMH Policy #95-6.

II. SCOPE OF POLICY:

This Policy only applies to DMH Computerized Information Systems containing DMH Client Records or Data and to the Users of such Systems.

III. DEFINITIONS:

- Audit Trail: A system produced report of all individuals gaining access to the system within a period of time. At a minimum, it includes all authorized logons and all unauthorized and/or unsuccessful logon attempts. Additionally, it may report to some degree the specific data that was accessed by a User or an unauthorized individual while logged-on.
- DMH Client Record: Any data element or collection of data elements that can be readily or Data: associated with a particular DMH Client (e.g., name, address, date of birth and social security number).
- DMH Computerized Information System: An information system owned or operated by DMH in which data are entered, stored or retrieved in a computer or in electronically controlled or accessible files.
- Data Integrity: The procedures and means for ensuring the correctness, validity and reliability of information.
- Disaster Recovery: The procedures and means for ensuring that a DMH Computerized Information System will recover quickly after a disaster with a minimum amount of information loss.
- DMH Client: Any person who is applying for, receiving, or has received services provided or contracted for by DMH.
- Security Administrator: A DMH employee responsible for administering security functions associated with a DMH Computerized Information System, such as processing authorized Users' access to the system, conducting system audits, assigning passwords, researching unauthorized access and preventing virus programs from entering the system.
- Perimeter Control: The procedures and means for protecting a Computerized Information System from unauthorized users and ensuring authorized Users' remote access.
- Physical Security: Non-systems oriented procedures used to control and Security safeguard access to a DMH Computerized Information System, e.g., controlling access to areas containing computer equipment and securing unattended terminals.
- User: Any individual who is authorized to use a DMH Computerized Information System.

IV. ADMINISTRATIVE POLICY AND PRACTICES:

A. Need to Know Standard: Access to a DMH Computerized Information System must be limited to Users whose job responsibilities or functions require the information contained on the system. When access is granted to a User, it shall be limited, to the extent possible, to that information that is absolutely necessary to enable the User to do his or her job.

B. Minimum Security Requirements for a DMH Computerized Information System: A DMH Computerized Informational System at a minimum must have the ability, through the system, to

1. Limit access to Users;
2. Produce Audit Trails;
3. Ensure Data Integrity;
4. Detect and eliminate potential virus programs; and
5. Allow for appropriate Perimeter Control.

C. Security Administrator: The Central Office and each DMH Area Office shall assign a Security Administrator (SA) to be responsible for maintaining security and confidentiality of DMH Computerized Information Systems in accordance with this policy and any guidelines developed pursuant to this policy. An Area may assign additional SAs as needed. SAs are to:

1. Process and control authorizations by overseeing the granting, renewing, and terminating of access to a DMH Computerized Information System;
2. Administer User system IDs and authorizations, such as establishing, disabling and monitoring logon IDs, passwords and system logon attempts;
3. Ensure that security needs are identified, and breaches investigated and reported to the Site Manager, Area Director, and/or the Commissioner, as appropriate;
4. Develop and implement corrective action plans associated with identified security issues;
5. Conduct audits of DMH Computerized Information System Users to assess the degree of compliance with this policy and any applicable guidelines developed pursuant to this policy. Audits shall include the periodic review of Audit Trail logs or other mechanisms that monitor User and unauthorized individuals' access. The results of each audit shall be forwarded to the Commissioner or responsible Area Director, for further review, and filed for further reference.
6. Communicate with the local Human Resource office to keep informed of employee terminations, hires, promotions, and transfers in order to adjust or terminate User access, as appropriate;
7. Answer questions regarding the DMH Security and Confidentiality Policy from Users and DMH Clients; and
8. Prevent virus programs from entering the System.

D. Confidentiality and Security Training Plan: The Central Office and each Area Office shall establish and implement a training plan to ensure that Users understand and respect the confidentiality of DMH Client Records and Data. Training must include a review of applicable federal and state laws and regulations, DMH policies and guidelines and the applicable DMH Computerized Information Systems' security controls. The training plan must provide for periodic training and shall be flexible enough to allow for the timely training of new Users. The training plan shall be reviewed periodically and updated as necessary.

E. Client Records and Data: Access to DMH Client Records and Data maintained on a DMH Computerized Information System is governed by the Department's regulations that govern Client Records and Data in general.

F. Data Maintenance: The maintenance of DMH Computerized Information System records are subject to the same laws, regulations, and protocols that are applicable to hard copy records of the same type.

G. Data Exchange: The integration or interface of a DMH Computerized Information System with a non-DMH Computerized Information System may be allowed only if the other system can sufficiently control security of its computerized data and such exchange as is otherwise permitted by law.

H. User Requirements:

1. Passwords: Users are required to select and safeguard their individual passwords to gain system access. A password may not be shared among Users.
2. Confidentiality and Security Training: To be authorized to have access to a DMH Computerized Information System an individual must have attended a DMH Confidentiality and Security Training Program as described in Section IV.D. of this policy. Proof of attendance shall be filed in the User's personnel file.
3. Limited Use: Users must limit their use of a DMH Computerized Information System to the legitimate purposes for which it is designed and for which their job responsibility requires access.
4. Adherence to all Applicable Laws: Users must adhere to all applicable federal and state laws

and regulations and DMH policies governing system security and client confidentiality.

5. Penalties Associated with Breaching Confidentiality: Users found to have violated any law, regulation or policy governing confidentiality may be subject to disciplinary action, including termination of employment, and legal action.

I. System Guidelines: Specific security guidelines must be developed for each DMH Computerized Information System. The Commissioner, or designee, shall be responsible for ensuring that guidelines are developed and implemented for any system that operates on a statewide basis and Area Directors, or designees, shall be responsible for ensuring that guidelines are developed for systems that operate only on an Area basis. These guidelines shall be periodically reviewed and updated as needed. At a minimum, a guideline shall include:

1. Need to Know List. This is a list by job titles or positions of the individuals whose job responsibilities or functions require access to the information contained in the system and who may, therefore, be authorized for access;
2. The range of access (e.g., statewide, Area, local) and the type of data (e.g., demographic, clinical) each of the job titles or positions included on the Need to Know List can be given;
3. Access authorization procedures (required sign-offs)
4. The length of time DMH Client Records and Data should be kept active on the system and procedures for archiving Client Records and Data from the system;
5. Conversion of current and historical Client Records and Data from an existing to a new system;
6. Data Integrity;
7. Disaster Recovery;
8. Perimeter Control;
9. Physical Security; and
10. Required Audit Trails and audit reports for the system (including the frequency, contents, reviewer, etc.)

V. POLICY IMPLEMENTATION:

Responsibility for the implementation of this policy is as follows:

A. The Commissioner or designee shall be responsible for ensuring compliance with this policy at the Central Office and statewide level and shall review and approve specific implementation guidelines for all DMH Computerized Information Systems.

B. The Area Directors shall be responsible for compliance with this policy in each Area.

VI. REVIEW OF THIS POLICY:

This policy and its implementation shall be reviewed at least annually.